(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 April 2001 (05.04.2001)

PCT

(10) International Publication Number
WO 01/24560 A1

(51) International Patent Classification[7]: H04Q 7/38

(21) International Application Number: PCT/GB00/03702

(22) International Filing Date: 27 September 2000 (27.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9922847.0 27 September 1999 (27.09.1999) GB

(71) Applicant *(for all designated States except US)*: **SIMOCO INTERNATIONAL LIMITED** [GB/GB]; P.O. Box 24, St. Andrews Road, Cambridge CB4 1DP (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **RAYNE, Mark, Wentworth** [GB/GB]; 5 St. James Close, Stretham, Nr. Ely, Cambridgeshire CB6 3ND (GB).

(74) Agent: **FRANK B. DEHN & CO.**; 179 Queen Victoria Street, London EC4V 4EL (GB).

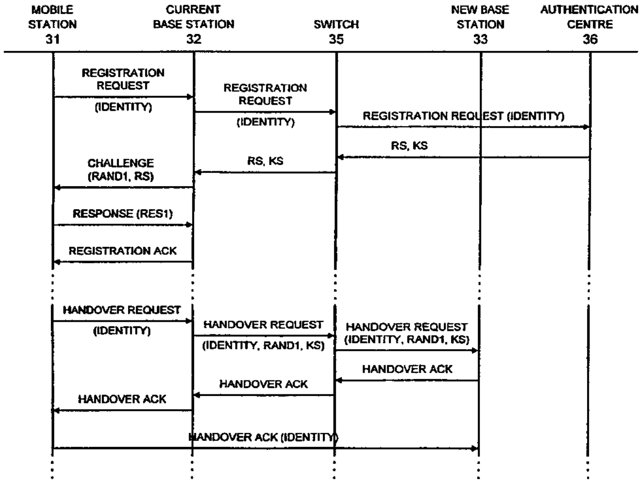
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: RADIO COMMUNICATIONS



(57) Abstract: A technique for the handover of a mobile station (30, 31, 44, 45) between base stations (32, 33, 39, 40) in a radio communications system in which the mobile stations and base stations each derive an encryption key (DCK) for encrypting their communications to each other. On handover, the key derivation parameters used by a mobile station to derive the encryption key are passed to the new base station, which then uses the parameters to re-derive the encryption key. The mobile station can then communicate with the new base station using the original encryption key for that call. Preferably the new base station seeks the key derivation parameters for a particular mobile station from a database. The key derivation parameters passed to the new base station on handover preferably comprise only parameters previously transmitted over the air-interface. In this way handover of a mobile station between base stations is achieved, without passing of the air-interface encryption key over the air-interface.

Radio Communications

The present invention relates to radio communications systems, and in particular to the encryption of transmissions in mobile radio communications systems.

In modern radio systems there is usually a requirement for encryption of the air interface (i.e. of the radio link between a mobile station and a base station) to deter eavesdroppers. In many radio systems the encryption key to be used is derived during operation of the mobile radio system by the mobile station and base station when they, for example, first communicate with each other. This encryption key derivation process will typically use corresponding algorithms in the base station and mobile station and a number of common parameters provided to and/or generated by the base station and mobile station.

For the convenience and security of radio system users and operators, the derivation of the encryption key is often combined with the process of authenticating the mobile station to the system. (As is known in the art, there is usually a requirement for authentication of a mobile station to the radio system to prevent unauthorised users from defrauding the system operator or misleading other users. There is also, increasingly, a requirement to make the authentication mutual, i.e. to allow a mobile station user to be assured that his or her radio unit is communicating with a base station belonging to the radio system.)

In such an arrangement, the secret key which is employed to operate the authentication algorithms is typically also used to generate a new, random individual encryption key each time the user authenticates with the system. This individual encryption key is then used by the mobile station to encrypt all further radio communications with the radio system over the air interface until a new authentication process takes place.

(The actual way that this individual encryption key is used will depend on the actual encryption process being employed. For example, in a block cipher it will typically be combined in some way with another input bit stream (which would typically be pseudo-random or at least unlikely to be repeated and change frequently during the encryption process (unlike the encryption key which can and typically will stay the same during the encryption process); this input bit stream is often referred to as an "initialisation vector" or "synchronisation vector"). The result of the combining of the encryption key and the initialisation vector bit stream (which is often referred to as a "key stream sequence" or "segment") is then used to encrypt the plain text (e.g. by being XORed with it).)

GSM (Global System for Mobile communications), DECT (Digital Enhanced Cordless Telephony) and TETRA (TErrestrial Trunked RAdio) systems all employ variants of this authentication and encryption key derivation mechanism. *Terrestrial Trunked Radio (TETRA) Voice plus Data (V+D)*; Part 7: Security, EN 300 392-7, European Telecommunications Standards Institute, F-06921 Sophia Antipolis, CEDEX - FRANCE describes this process for a TETRA system. Mouly, M, Paulet, M, *The GSM System for Mobile Communications*, Cell & Sys., 4 rue Elisee Reclus, F-91120 Palaiseau, France, 1992, ISBN 2-9507190-0-7 describes this process for a GSM radio system.

Figure 1 illustrates a known method of authenticating a mobile station 2 to a base station 3 in a mobile radio system. The TETRA system, for example, uses this form of authentication process (see, e.g. EN 300 392-7, section 4). To facilitate the authentication process, a secret authentication key 'K' is shared by the mobile station 2 and an 'authentication centre' 1. Authentication key K is not known by the base station 3, and should never be revealed outside the authentication centre and the mobile station.

When the base station 3 wishes to prove the authenticity of the mobile station, it requests a pair of values, random seed RS and session key KS, from the authentication centre 1. The authentication centre generates random seed RS, and inputs random seed RS and secret authentication key K into a one-way encryption algorithm TA11 to produce a session key KS (step 4 in Figure 1). Session key KS and random seed RS are then delivered to the base station 3 (step 9). The properties of encryption algorithm TA11 are such that is should be difficult to deduce authentication key K from a knowledge of random seed RS and session key KS.

The base station 3 then generates its own random number RAND1 and sends an authentication challenge to the mobile station 2 (step 10). Random number RAND1 and random seed RS are carried in the challenge message. Mobile station 1 derives its version of the session key KS using the delivered value of random seed RS and its copy of secret key K using encryption algorithm TA11 (step 5). The mobile station now combines its derived session key KS and the challenge random number RAND1 in an encryption algorithm TA12 to create a response RES1, which it transmits back to the base station 3 (step 6).

The base station also uses the session key KS it received from the authentication centre 1, the random number RAND1 and the encryption algorithm TA12 to create its version of the response, XRES1 (step 7). It then compares its value of the response, XRES1, with the value RES1 received from the mobile station. If the two agree, the base station can conclude that the mobile station and the authentication centre must share the same secret key K. The mobile station is therefore authenticated.

The authentication process is also used to derive a cipher key that is actually used for the encryption of (traffic) communications between the base station and mobile station. This is achieved by encryption algorithm TA12 generating a derived cipher (encryption) key, DCK1, at the same time as it produces response RES1 in the mobile station and as it produces response XRES1 in the base station. An authentic mobile station will, as will be appreciated from the above, derive the same cipher key as the base station. The derived cipher key DCK1 can then be used as an encryption key for air interface encryption between the mobile station and the base station. It should be noted that the derived cipher key DCK1 is in this arrangement never revealed outside the mobile station and the base station.

Figure 2 illustrates a known mutual authentication process. This type of process is again used, for example, in the TETRA system. In this case the authentication centre 11 and the mobile station 12 apply random seed RS and authentication key K to a second encryption algorithm TA21 to generate a second session key KS' (steps 18, 19 in Figure 2). Random seed RS and first and second session keys KS, KS' are sent to the base station 13 by the authentication centre (step 20).

As before, random number RAND1 and random seed RS are sent to the mobile station by the base station in a challenge (step 10), and as before the mobile station returns its derived response RES1 and also derives a cipher key DCK1 (step 6). If response RES1 agrees with response XRES1 derived in the base station, the base station can authenticate the mobile station.

However, in this case, to enable the mobile station 12 to authenticate the base station 13, the mobile station 12 generates and sends a new challenge random number RAND2 to the base station with its response RES1. The base station encrypts random number RAND2 in a further encryption algorithm TA22 using the second session key KS' to create response RES2 (step 17), and sends response RES2 to the mobile station. The mobile station computes its version of the response, XRES2, using algorithm TA22, random number RAND2 and its derived second session key KS' (step 15), and compares the two response values. If they are the same, the mobile station can conclude that the base station is in contact with the authentication centre which shares the mobile station's secret key, and authenticate the base station.

In this mutual authentication arrangement, encryption algorithm TA22 also generates a second derived cipher key, DCK2, and this is combined with the first derived cipher key, DCK1, in a further algorithm TB4 by both the mobile station and the base station to generate a (overall) derived cipher key, DCK (step 14, 16). This final derived cipher (encryption) key will again be the same if both the base station and mobile station are legitimate and can then be used for air-interface traffic encryption by both the mobile station and the base station.

While it is generally convenient to derive the air-interface encryption (cipher) key in use when a mobile station first communicates with a new base station, e.g. as part of the authentication process, the Applicants have recognised that in certain circumstances such an arrangement may not always be convenient. For example, when a mobile station wishes to move (i.e. handover) from one radio base station to another while engaged in a call, it is generally required that such a 'handover' be seamless, i.e. undetectable to the user. However, the encryption key derivation (e.g. authentication) process may take some time to complete and thus a seamless handover may not be possible if a new encryption key has to be derived (e.g. the mobile station has to be authenticated at the new base station) before it can continue its conversation.

Thus if seamless handover is required, such that it is necessary to defer key derivation, e.g. authentication, at the new base station, the derived air interface encryption key (i.e. the key which is being used by the mobile station to encrypt traffic) which was in use between the mobile station and the first base station must be used in communications between the mobile station and the second, new base station. This in turn means that second base station must be made aware of the encryption key at the time that the handover is requested.

One way to do this would be simply to pass the originally derived air interface encryption key currently in use from the first base station to the second base station. However, transferring encryption keys between base stations is hazardous, as an interceptor of a communications link from one of the base stations could be able to obtain the key. This may then compromise not only communication between the mobile station and the current base station, but also radio communications between the mobile station and other base stations to which it is handed.

Furthermore, a mobile station's personal derived air interface encryption key is often used to encrypt for transmission other encryption keys to be used in the radio system, as in many radio systems it is often necessary to deliver further encryption keys over the air-interface.

For example, the TETRA system uses a common cipher key (CCK) for common use by plural mobile stations which is used by mobile stations for encrypting their identity, and for decrypting messages addressed to local call groups of which they are a member, a group cipher key (GCK) which is an additional key for group communications where the common cipher key alone does not provide sufficient protection and for use in group calls throughout the radio system, and static cipher keys (SCK) which are for direct mode operation (i.e. communication independently of a fixed radio network). These additional cipher keys are typically delivered to a mobile station over the air interface, and the mobile station's current derived air interface cipher key would usually be used to encrypt (seal) these keys when they are being delivered.

Thus, interception of one mobile station's derived air interface cipher key may also enable the interceptor to obtain access to additional encryption keys in use by other mobile stations.

It would be possible to encrypt the derived air interface encryption (cipher) key before sending it from one base station to another. However, the use of encrypted communication links means additional keys are required. If symmetric encryption is used either a common key must be used for all inter-base station encryption key exchanges, or a separate key must be held for each pair of base stations. If asymmetric encryption is used, each base station would have its own public key-private key pair, and a list of the public keys of all the nearby base stations to which hand-over might be required.

However, implementing such encryption of base station links would introduce additional key management problems and processing overheads, and is not therefore necessarily desirable.

According to a first aspect of the present invention, there is provided a method of operating a mobile radio communications system, which system comprises one or more mobile stations and plural base stations, and wherein the mobile stations and base stations of the system each carry out an encryption key derivation process using one or more key derivation parameters to derive an encryption key for encrypting their communications to each other, the method comprising:

when a mobile radio unit is handed over from one base station to another during an on-going call, passing one or more of the key derivation parameters used by the mobile station to derive the encryption key being used for the call to the new base station, and

the new base station using the key derivation parameters it receives to derive the encryption key to be used for the call.

According to a second aspect of the present invention, there is provided a mobile radio communications system, comprising

one or more mobile stations;

a plurality of base stations;

the mobile stations and base stations each comprising means for deriving an encryption key for encrypting their communications to each other from one or more key derivation parameters;

the system further comprising:

means for, when a mobile station is handed over to another base station during an on-going call, passing to the new base station, one or more of the key derivation parameters used by the mobile station to derive the encryption key being used for the call, whereby the new base station can derive the encryption key to be used for the call.

In the present invention, when handover occurs during an on-going call, one or more of the encryption key derivation parameters used to derive the air interface encryption (cipher) key being used for the call are passed to the new base station which then uses those parameters to derive the air interface encryption key to be used for the call. This allows the mobile station to continue to use its existing air interface encryption key in its communications with the new base station, and thus there is no need for the mobile station and new base station to derive a new air interface encryption key for their communications, thereby allowing a more seamless handover. Furthermore, there is no need to transfer the existing air interface encryption key itself to the new base station. Thus that key is not revealed outside the base and mobile stations and there is also no need for the additional encryption arrangements that such revelation might entail.

Thus in the present invention the existing air interface encryption key being used for the call is not itself passed to the new base station, but the new base station can still derive that key and then use it for the call. This is achieved by passing key derivation parameters to the new base station to enable it to derive the encryption key to be used for the call. As it is the parameters required to derive the encryption key, rather than the key itself, which are transferred between the base stations, the present invention can thus effectively transfer the original encryption key used for the call between base stations, but in a manner which renders encryption of keys unnecessary, thereby avoiding additional key management and processing problems.

The encryption key derivation process can be any suitable such process. It would normally use predetermined key derivation algorithms (with all of the mobile stations and base stations of the system preferably using the same, predetermined encryption key derivation process), but the key derivation parameters may be randomly generated, and/or predetermined and unique to a given mobile station, and/or, at least initially, supplied from another location, such as an authentication centre.

The encryption key derivation process would normally take place when a mobile radio unit first contacts a base station (except when it does so during an ongoing call and is operating in accordance with the present invention). It will typically be a mobile station and/or base station authentication process as discussed above. In such an arrangement in the present invention the new base station would therefore effectively use the key derivation mechanism employed during the authentication process to derive the air interface encryption key, using the one or more of the key derivation parameters passed to it to enable it to do so.

The key derivation parameters may be passed to the new base station as desired. They are preferably passed to the new base station by the existing base station, as this would usually be more convenient, but the mobile station may pass the encryption key derivation parameters to the new base station if desired. The key derivation parameters are preferably passed to the new base station with the handover request (e.g. by the existing base station as soon as it receives the handover request from the mobile station or decides itself to perform a handover).

In one preferred embodiment, the key derivation parameters are passed to the new base station over communication links that they would normally be passed over in the normal key derivation process, as this introduces no new security considerations over and above the security risks already present in the derivation process.

The key derivation parameters passed to the new base station should be those parameters such as are necessary for it to derive the encryption key to be used for the call. They would typically be or include one or more of the original key derivation parameters used to derive the encryption key to be used for the call by the mobile station and/or the first base station.

Thus for example, in a key derivation process that uses derived session keys and a challenge random number to derive the air interface or traffic encryption key, such as in the authentication and key derivation processes discussed in detail above, it would, for example, be sufficient to pass the session key or keys and challenge random number or numbers (i.e. in the above example session key KS and the challenge random number RAND1, where only the mobile station is authenticated, or the session keys KS and KS' and the challenge random numbers RAND1 and RAND2 where mutual authentication is being used) to the new base station for it to derive the derived air interface encryption key using the key derivation algorithms (algorithm TA12, or algorithms TA12, TA22 and TB4, respectively, in the above examples), which algorithms the new base station will already know.

In a particularly preferred embodiment, the key derivation parameters sent to the new base station comprise only parameters that have already been transmitted over the air-interface, as in that case no new security risk would be introduced by sending them across an unencrypted communications link (such as an unencrypted mobile station to base station air interface or a microwave link between the base stations) to the new base station (and would therefore permit the use of an unencrypted communications link for such parameter transfer). The new base station could then, if necessary, seek further necessary key derivation information from another source.

In a preferred embodiment therefore a record is kept of key derivation parameters previously used for a given mobile radio unit, so as to allow those parameters to be retrieved if necessary by a new base station communicating with that mobile radio unit. The parameters should be stored in a database or databases accessible by base stations of the fixed radio network, and record the parameters against each mobile radio unit's identity to allow them to be retrieved. A single central database could be used, which could, for example, be at the authentication centre.

Alternatively, plural copies of the relevant key derivation parameters and mobile station identity records could be stored at plural different locations in the fixed radio network. This may help to avoid delays due to bottlenecks in the network when many base stations are seeking the records at the same time.

Thus, for example, in a key derivation process that uses a random seed to derive a session key or keys that are used, together with challenge random number(s), to derive the air-interface encryption key, such as the authentication and key derivation process exemplified above, the values of the random seed and challenge random number or numbers (i.e. in the above examples the random seed RS, the random number RAND1 and, if necessary the random number RAND2) could be sent to the new base station. The new base station could then, for example, obtain the values of session key or keys (in the above example the session key or keys KS and KS') that it needs to derive the encryption key by seeking them from the stored key derivation parameter records.

In this arrangement, to allow the key derivation parameter store to know which session keys to send to the new base station, each session key or key set could be recorded with the corresponding random seed value and mobile station identity (since these parameters will identify the relevant sessions keys) in the store. The new base station is provided with the mobile station's identity and the relevant random seed value and can thus transmit them to the key derivation parameter store which can then retrieve the corresponding values of the session key or keys from its records and send them to the new base station which will then be able to derive the original derived encryption key. Thus, in one arrangement, the generated session key or keys, KS and KS', and corresponding random seed RS generated for a particular mobile station are stored along with the mobile station's identity, so that they can be retrieved at a later date.

It is believed that recording encryption key derivation parameters to allow them to be retrieved for use by a base station that did not receive them when they were first derived may be advantageous in its own right. Thus, according to a third aspect of the present invention, there is provided a method of operating a mobile radio communications system in which system during an authentication procedure for a mobile radio unit using the system, a random seed value is used to derive a session key or keys for use to derive a cipher key for use for air-interface encryption, the method comprising storing in a database a record for the or each mobile radio unit of random seed values and the corresponding session keys previously used for that mobile radio unit.

According to a fourth aspect of the present invention, there is provided a mobile radio communications system, in which system during an authentication procedure for a mobile radio unit using the system, a random seed value is used to derive a session key or keys for use to derive a cipher key for use for air-interface encryption, the system comprising means for storing in a database a record for the or each mobile radio unit of random seed values and the corresponding session keys previously used for that mobile radio unit.

In an alternative arrangement, the new base station could provide the mobile station's identity and the random seed value to the authentication centre, which could then use the mobile station's secret authentication key K and the random seed value to rederive the session key or keys.

Thus, according to a fifth aspect of the present invention, there is provided a method of operating a mobile radio communications system, in which system during an authentication procedure for a mobile radio unit using the system, an authentication centre of the system generates and uses a random seed value to derive a session key or keys for use by the mobile radio unit and a base station of the system to derive a cipher key for use for air-interface encryption by the mobile radio unit, the method comprising:

the mobile radio unit or a base station of the system returning a generated random seed value together with the identity of the mobile radio unit to the authentication centre;

the authentication centre, on the basis of the random seed value and mobile radio unit's identity provided to it, rederiving the session key or keys originally derived using that random seed value for the mobile radio unit; and

the authentication centre providing the rederived session key or keys to another base station of the system to allow that base station to derive the cipher key.

Thus, according to a sixth aspect of the present invention, there is provided a mobile radio communications system, comprising:

plural mobile radio units;

plural base stations;

an authentication centre for carrying out an authentication procedure for a mobile radio unit using the system, which authentication centre comprises means for, during the authentication procedure, generating and using a random seed value to derive a session key or keys for use by the mobile radio unit and a base station of the system to derive a cipher key for use for air-interface encryption by the mobile radio unit; in which system:

the mobile radio units and/or base stations of the system comprise means for returning a generated random seed value together with the identity of a mobile radio unit to the authentication centre;

the authentication centre comprises means for, on the basis of the random seed value and mobile radio unit's identity provided to it, rederiving the session key or keys originally derived using that random seed value for the mobile radio unit, and means for providing the rederived session key or keys to another base station of the system to allow that base station to derive the cipher key.

The methods in accordance with the present invention may be implemented at least partially using software e.g. computer programs. It will thus be seen that when viewed from a further aspect the present invention provides computer software specifically adapted to carry out the methods hereinabove described when installed on data processing means and a computer program element comprising computer software code portions for performing the methods hereinabove described when the program is run on data processing means. The invention also extends to a computer software carrier comprising such software which when used to operate a radio system or base station or mobile station comprising a digital computer causes in conjunction with said computer said system or station to carry out the steps of the method of the present invention. Such a computer software carrier could be a physical storage medium such as a ROM chip, CD ROM or disk, or could be a signal such as an electronic signal over wires, an optical signal or a radio signal such as to a satellite or the like.

It will further be appreciated that not all steps of the method of the invention need be carried out by computer software and thus from a further broad aspect the present invention provides computer software and such software installed on a computer software carrier for carrying out at least one of the steps of the methods set out hereinabove.

A number of preferred embodiments will now be described by way of example only, and with reference to the accompanying drawings, in which:

Figure 1 illustrates the authentication of a TETRA mobile station;

Figure 2 illustrates mutual authentication in the TETRA system;

Figure 3 illustrates schematically one arrangement of a mobile radio system operating in accordance with the present invention;

Figure 4 illustrates schematically another arrangement of a mobile radio system operating in accordance with the present invention;

Figure 5 is a message sequence chart showing one embodiment of a messaging sequence for a mobile radio system operating in accordance with the present invention; and

Figure 6 is a message sequence chart showing another embodiment of a messaging sequence for a mobile radio system operating in accordance with the present invention.

Two examples of the operation of a mobile radio system in accordance with the present invention will now be described.

Figures 3 and 5 show the first example in which mobile station 30 wishes to call mobile station 31 (which communicates with the fixed radio network via base station 34) (see Figure 3). Figure 5 is a message sequence chart showing the exchange of messages as the call progresses.

When it wishes to make the call, mobile station 30 first registers with base station 32. The base station 32 passes the call request on to the authentication centre 36, via switch 35. Authentication of the mobile station 30 then proceeds as described above with reference to Figure 1. (For simplicity, a one-way authentication is illustrated).

Thus, authentication centre 36 supplies session key

KS and random seed RS to base station 32 via switch 35. Base station 32 generates random number RAND1 and sends random number RAND1 and random seed RS to the mobile station 30 as a challenge. Mobile station 30 computes its response RES1 and returns it to base station 32. At the same time it derives an encryption (cipher) key, DCK, for use when communicating with base station 32, using random number RAND1, random seed RS, and its secret key K. The base station confirms that the mobile station's response RES1 is the correct response, derives its cipher key, DCK, from the session key KS and random number RAND1 (which cipher key should be the same as the mobile station's derived cipher key, DCK, where the mobile station is authentic), and acknowledges mobile station 30's registration request.

The mobile station and base station can then use the derived cipher key DCK to encrypt their communications to each other. This would typically be done by using the derived cipher key DCK in combination with a pseudo-random or at least varying input initialisation vector to generate a key stream sequence which is used to encrypt the plain text traffic to be sent. TETRA can use this form of encryption mechanism (see, e.g., ETSI EN 300 392-7, section 6).

Consider the case where, while engaged in a call with mobile station 31, mobile station 30 determines that it requires a handover from current base station 32 to new base station 33. Mobile station 30 sends its handover request to base station 32. (In a TETRA system, the mobile stations determine when a handover is necessary; in GSM the base stations make the decision, but this difference is immaterial to the present invention.) Base station 32 sends the handover request to base station 33 via switch 35.

As discussed above, a derived cipher key must be used for communications between the mobile station 30 and the new radio base station 33. However, the originally derived cipher key DCK in use between mobile station 30 and base station 32 is unknown outside the mobile station 30 and the base station 32. Thus either the mobile station 30 has to re-authenticate at the new base station 33, to derive a new cipher key, or the old cipher DCK must be used at the new base station. If seamless handover is required, there is no time to re-authenticate, and the second method must be used.

Thus, in accordance with the present invention, the handover request message from base station 32 to base station 33 contains the identity of mobile station 30, and the values of random number RAND1 and session key KS used to derive the cipher key that mobile station 30 is currently using. Base station 33 regenerates the cipher key DCK using random number RAND1 and session key KS in algorithm TA12 (Figure 1) and sends a message to base station 32 via switch 35. Base station 32 confirms the handover request to mobile station 31. Mobile station 31 switches to a radio channel used by base station 33 and makes direct contact with base station 33, still using the cipher key DCK it was using with base station 33.

In this example, there is minimal interruption to the mobile station 30 by the handover signalling, and the derived cipher key is never exposed outside mobile station 31 and base stations 32 and 33. Session key KS is transmitted along the communication links from base station 32 and base station 33 to the switch 35. However, such session keys would normally be sent across such communications links during authentication, and thus the handover arrangement introduces no additional security hazards beyond those already present in the radio network and does not further endanger the derived cipher key used for air interface encryption.

Figures 4 and 6 show a further example of the operation of a radio system in accordance with the present invention, but in which system there is a direct radio link between base stations 39 and 40 via antennae 41 and 42. Mobile station registration and encryption key generation proceeds as before. Again, the case when, during a call to mobile station 45, it becomes necessary for mobile station 44 to be handed over to base station 40 will be considered.

This time, when handover is required, mobile station 44's handover request is sent directly to new base station via radio link 41-42. However, in this case, passing the session key KS to the new base station 40 via radio link 41-42 may be undesirable, as an interceptor of that link who has a knowledge of the key derivation algorithms (i.e., in the above example, of algorithms TA12, TA22, and/or TB4) would be able to recreate the derived cipher key.

Thus, instead of sending the session key KS, the base station 39 sends the mobile station 44's identity and the values of random number RAND1 and random seed RS used to derive the cipher key to the new base station 40 via radio link 41-42. Base station 40 now requests from authentication centre 37 via switch 38 the value of the session key KS corresponding to the identity of mobile station 44 and random seed RS. The authentication station recomputes session key KS using the secret key K and random seed RS, and returns session key KS to base station 40 via switch 38. Base station 40 can now derive the air-interface traffic cipher key, and acknowledges the handover request to base station 39 via radio line 41-42. Base station 39 signals the acknowledgement to mobile station 44, and mobile station 44 contacts base station 40 directly.

In this second example, neither the derived cipher key or session key KS are revealed over the radio link, yet the original derived cipher key is safely derived by base station 40, and a seamless handover is achieved. Session key KS is revealed only on communication links which already carry session key KS values for authentication purposes, so nothing new will be revealed to an interceptor.

Although the present invention has been described above with reference to the TETRA system, it is, as will be appreciated by those skilled in the art, applicable to any mobile radio system where encryption keys are derived in use by mobile stations and base stations, such as the GSM system.

Claims:

1. A method of operating a mobile radio communications system, which system comprises one or more mobile stations and plural base stations, and wherein the mobile stations and base stations of the system each carry out an encryption key derivation process using one or more key derivation parameters to derive an encryption key for encrypting their communications to each other, the method comprising:

when a mobile station is handed over from one base station to another during an on-going call, passing one or more of the key derivation parameters used by the mobile station to derive the encryption key being used for the call to the new base station, and

the new base station using the key derivation parameters it receives to derive the encryption key to be used for the call.

2. A method of operating a mobile radio communications system as claimed in claim 1 wherein the key derivation parameters are passed to the new base station with the handover request.

3. A method of operating a mobile radio communications system as claimed in any one of claims 1 or 2, wherein the key derivation parameters are passed to the new base station during the on-going call via the same communication links as used to pass key derivation parameters between a mobile station and a base station when a mobile station first contacts the base station not during an on-going call.

4. A method of operating a mobile radio communications system as claimed in any one of the preceding claims wherein a derived session key or keys and challenge random number or numbers are used to derive the

encryption key, further comprising passing the session key or keys and challenge random number or numbers used to derive the encryption key to the new base station.

5. A method of operating a mobile radio communications system as claimed in any one of the preceding claims wherein the key derivation parameters passed to the new base station on handover comprise solely parameters previously transmitted over the air-interface.

6. A method of operating a mobile radio communications system as claimed in any one of the preceding claims wherein the new base station seeks further key derivation information from a database.

7. A method of operating a mobile radio communications system as claimed in claim 6 wherein key derivation parameters previously used by mobile stations of the system are stored in association with a mobile station identifier in a database or databases accessible by base stations of the fixed radio network.

8. A method of operating a mobile radio communications system as claimed in claim 6 or 7 wherein a derived session key or keys and challenge random number or numbers are used to derive the encryption key, and a random seed is used to derive the session key or session keys, further comprising passing the random seed and challenge random number or numbers to the new base station, and the base station seeking the session key or keys from a database storing key derivation parameter information.

9. A method of operating a mobile radio communications system as claimed in claim 8, wherein the session key or key set and the corresponding random seed value are stored in the database in association with the mobile

station identifier.

10. A method of operating a mobile radio communications system as claimed in any one of the preceding claims, wherein during an authentication procedure for a mobile station using the system, an authentication centre of the system generates and uses a random seed value to derive a session key or keys for use by the mobile station and a base station of the system to derive a cipher key for use for air-interface encryption by the mobile station, further comprising passing an identifier for the mobile station in association with the random seed value to an authentication centre, further comprising the authentication centre using a common authentication key of the mobile station and base station with the random seed value to rederive the session key or keys and providing the rederived session key or keys to another base station of the system to allow that base station to derive the cipher key.

11. A method of operating a mobile radio communications system in which system during an authentication procedure for a mobile station using the system, a random seed value is used to derive a session key or keys for use to derive a cipher key for use for air-interface encryption, the method comprising storing in a database a record for the or each mobile station of random seed values and the corresponding session keys previously used for that mobile station.

12. A method of operating a mobile radio communications system, in which system during an authentication procedure for a mobile station using the system, an authentication centre of the system generates and uses a random seed value to derive a session key or keys for use by the mobile station and a base station of the system to derive a cipher key for use for air-interface

encryption by the mobile station, the method comprising:

the mobile station or a base station of the system returning a generated random seed value together with the identity of the mobile station to the authentication centre;

the authentication centre, on the basis of the random seed value and the mobile station identifier provided to it, rederiving the session key or keys originally derived using that random seed value for the mobile station; and

the authentication centre providing the rederived session key or keys to another base station of the system to allow that base station to derive the cipher key.

13. A mobile radio communications system, comprising

one or more mobile stations;

a plurality of base stations;

the mobile stations and base stations each comprising means for deriving an encryption key for encrypting their communications to each other from one or more key derivation parameters;

the system further comprising:

means for, when a mobile station is handed over to another base station during an on-going call, passing to the new base station, one or more of the key derivation parameters used by the mobile station to derive the encryption key being used for the call, whereby the new base station can derive the encryption key to be used for the call.

14. A mobile radio communications system, in which system during an authentication procedure for a mobile station using the system, a random seed value is used to derive a session key or keys for use to derive a cipher key for use for air-interface encryption, the system comprising means for storing in a database a record for

the or each mobile station of random seed values and the corresponding session keys previously used for that mobile station.

15. A mobile radio communications system, comprising:

plural mobile stations;

plural base stations;

an authentication centre for carrying out an authentication procedure for a mobile station using the system, which authentication centre comprises means for, during the authentication procedure, generating and using a random seed value to derive a session key or keys for use by the mobile station and a base station of the system to derive a cipher key for use for air-interface encryption by the mobile station; in which system:

the mobile stations and/or base stations of the system comprise means for returning a generated random seed value together with the identity of a mobile station to the authentication centre;

the authentication centre comprises means for, on the basis of the random seed value and mobile station's identity provided to it, rederiving the session key or keys originally derived using that random seed value for the mobile station, and means for providing the rederived session key or keys to another base station of the system to allow that base station to derive the cipher key.

16. A mobile radio communications system, as claimed in any one of claims 13 to 15 further comprising means for storing further key derivation information in a database.

17. Computer software specifically adapted to carry out the method of any one of claims 1 to 12 when installed on a data processing means.

18. A method of operating a mobile station of a mobile radio system, substantially as hereinbefore described with reference to any one of the accompanying drawings.

19. A method of operating a base station of a mobile radio system, substantially as hereinbefore described with reference to any one of the accompanying drawings.

20. A mobile station of a mobile radio system, substantially as hereinbefore described with reference to any one of the accompanying drawings.

21. A base station of a mobile radio system, substantially as hereinbefore described with reference to any one of the accompanying drawings.

22. A mobile radio communications system substantially as hereinbefore described with reference to any one of the accompanying drawings.

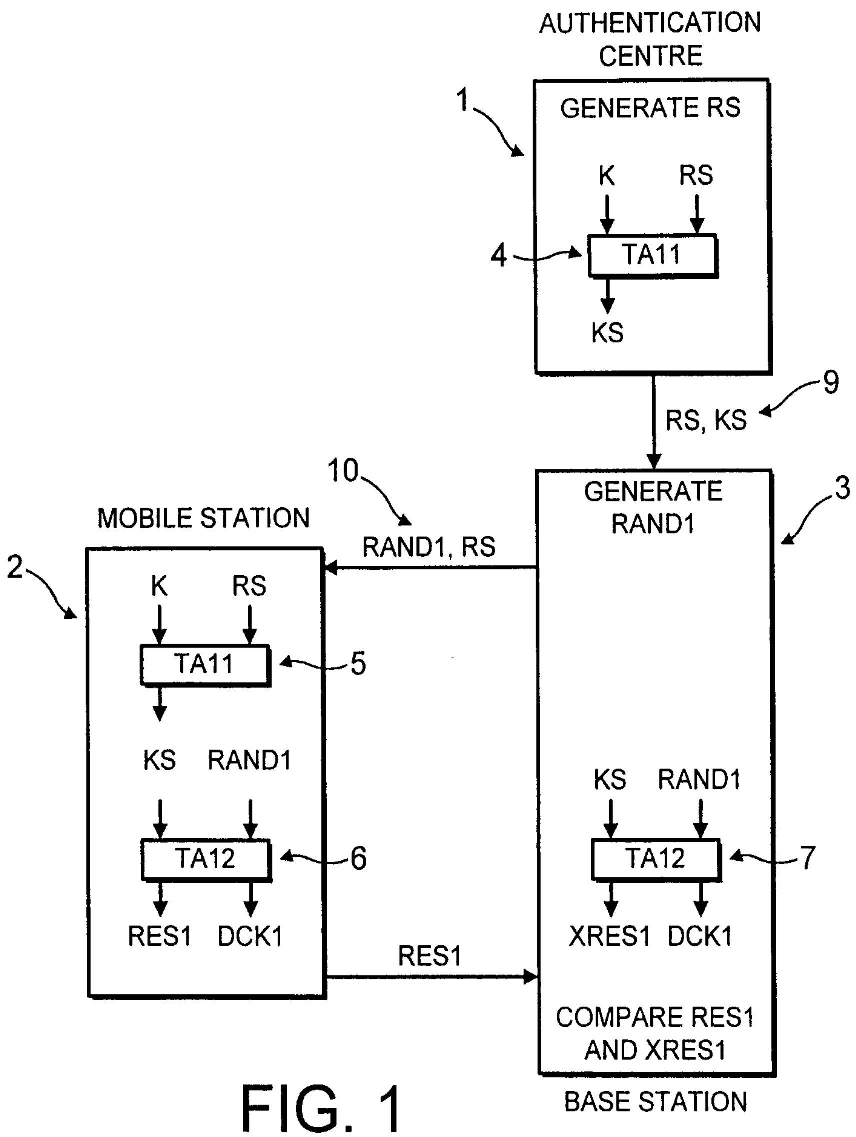

AUTHENTICATION CENTRE
1
GENERATE RS
K
RS
4
TA11
KS
9
RS, KS
10
GENERATE RAND1
3
MOBILE STATION
RAND1, RS
2
K
RS
TA11
5
KS
RAND1
TA12
6
RES1
DCK1
KS
RAND1
TA12
7
XRES1
DCK1
RES1
COMPARE RES1 AND XRES1
BASE STATION

FIG. 1

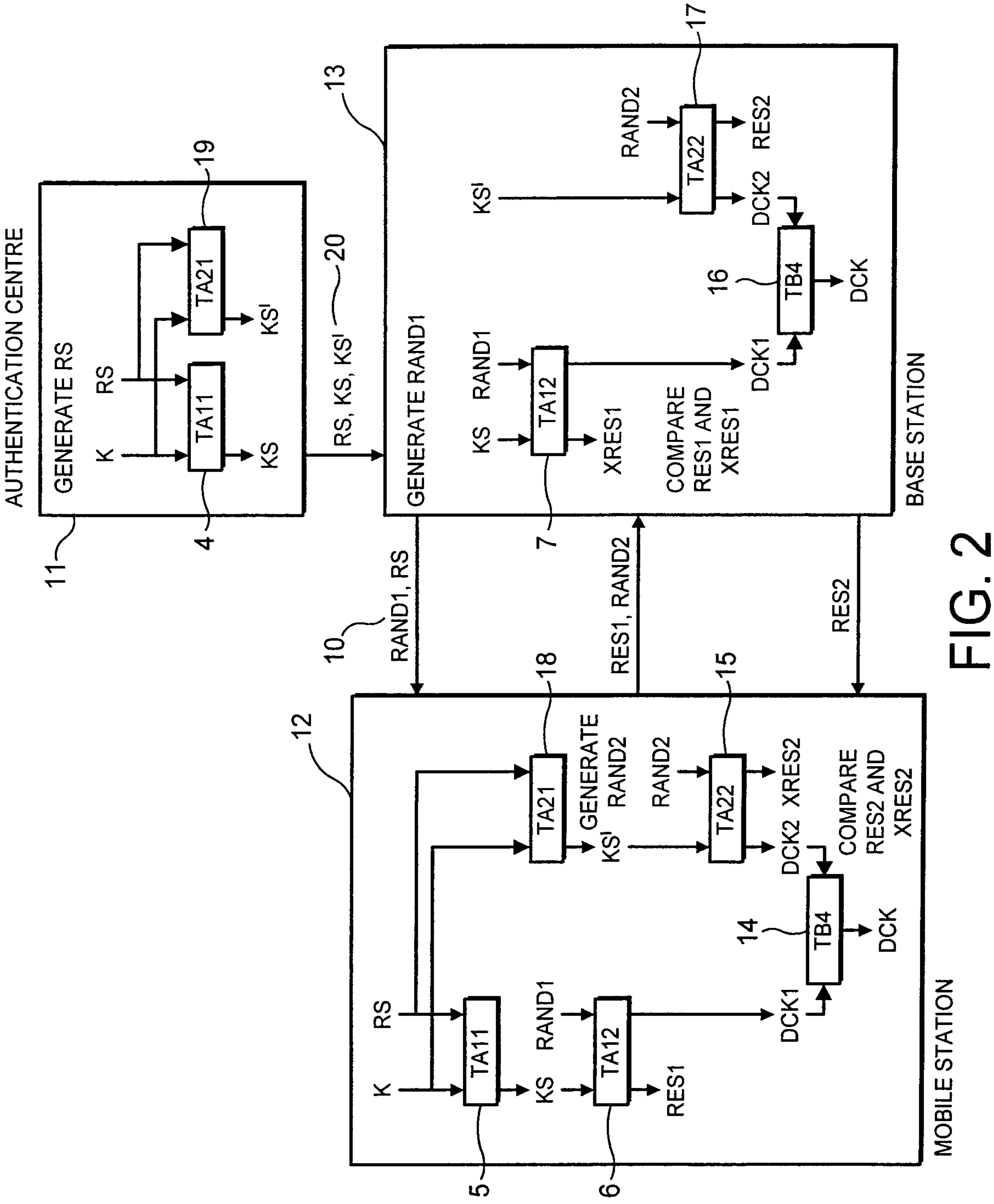

AUTHENTICATION CENTRE
GENERATE RS
K
RS
TA11
TA21
KS
KS'
11
4
19
RS, KS, KS'
20
13
GENERATE RAND1
KS
RAND1
TA12
XRES1
COMPARE RES1 AND XRES1
DCK1
KS'
RAND2
TA22
RES2
DCK2
17
TB4
16
DCK
7
BASE STATION
RAND1, RS
10
RES1, RAND2
RES2
12
K
RS
TA11
KS
RAND1
TA12
RES1
5
6
TA21
18
GENERATE RAND2
KS'
RAND2
TA22
15
XRES2
DCK2
COMPARE RES2 AND XRES2
TB4
14
DCK
DCK1
MOBILE STATION

FIG. 2

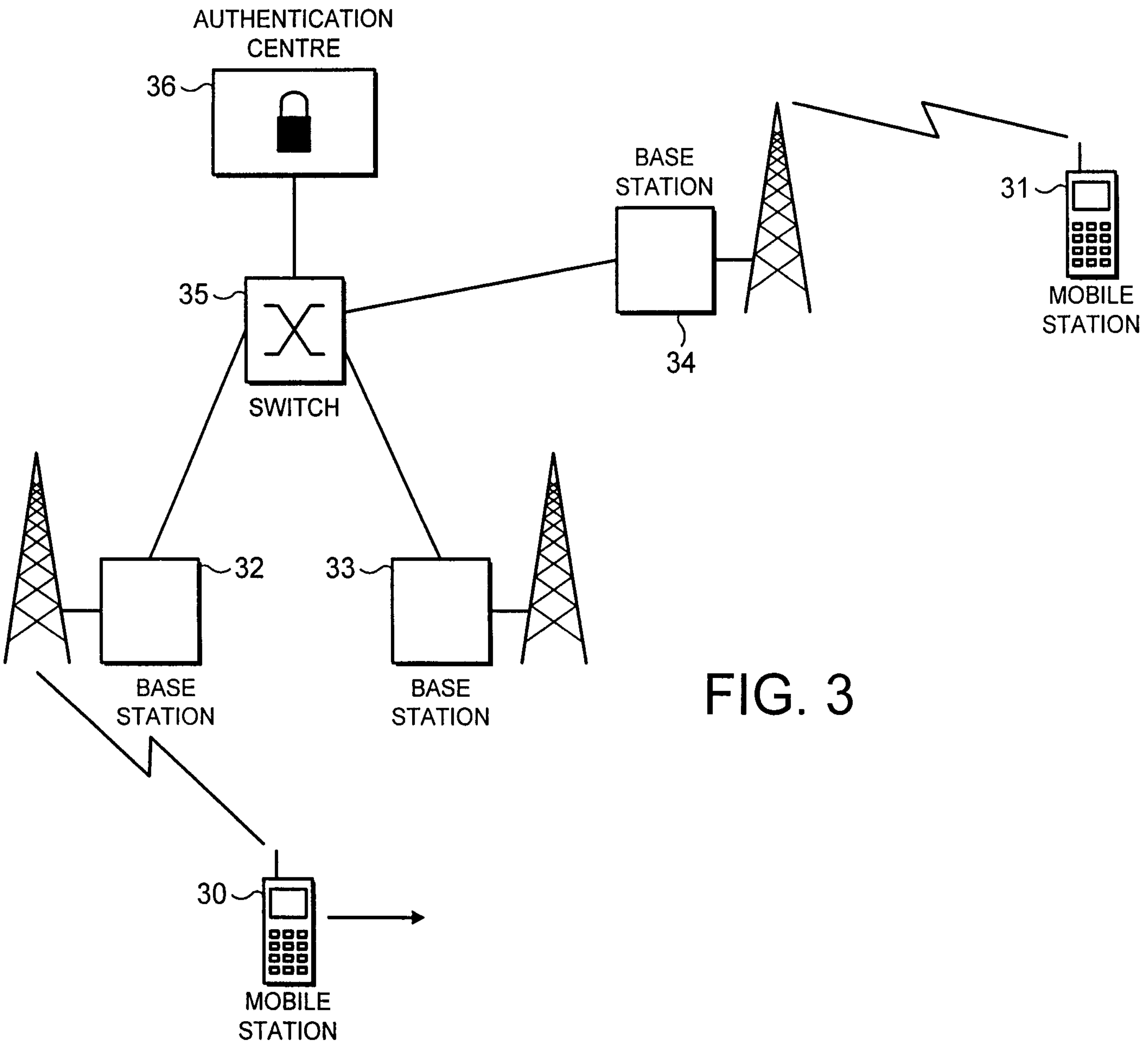

AUTHENTICATION
CENTRE
36
35
SWITCH
BASE
STATION
34
31
MOBILE
STATION
32
BASE
STATION
33
BASE
STATION
30
MOBILE
STATION

FIG. 3

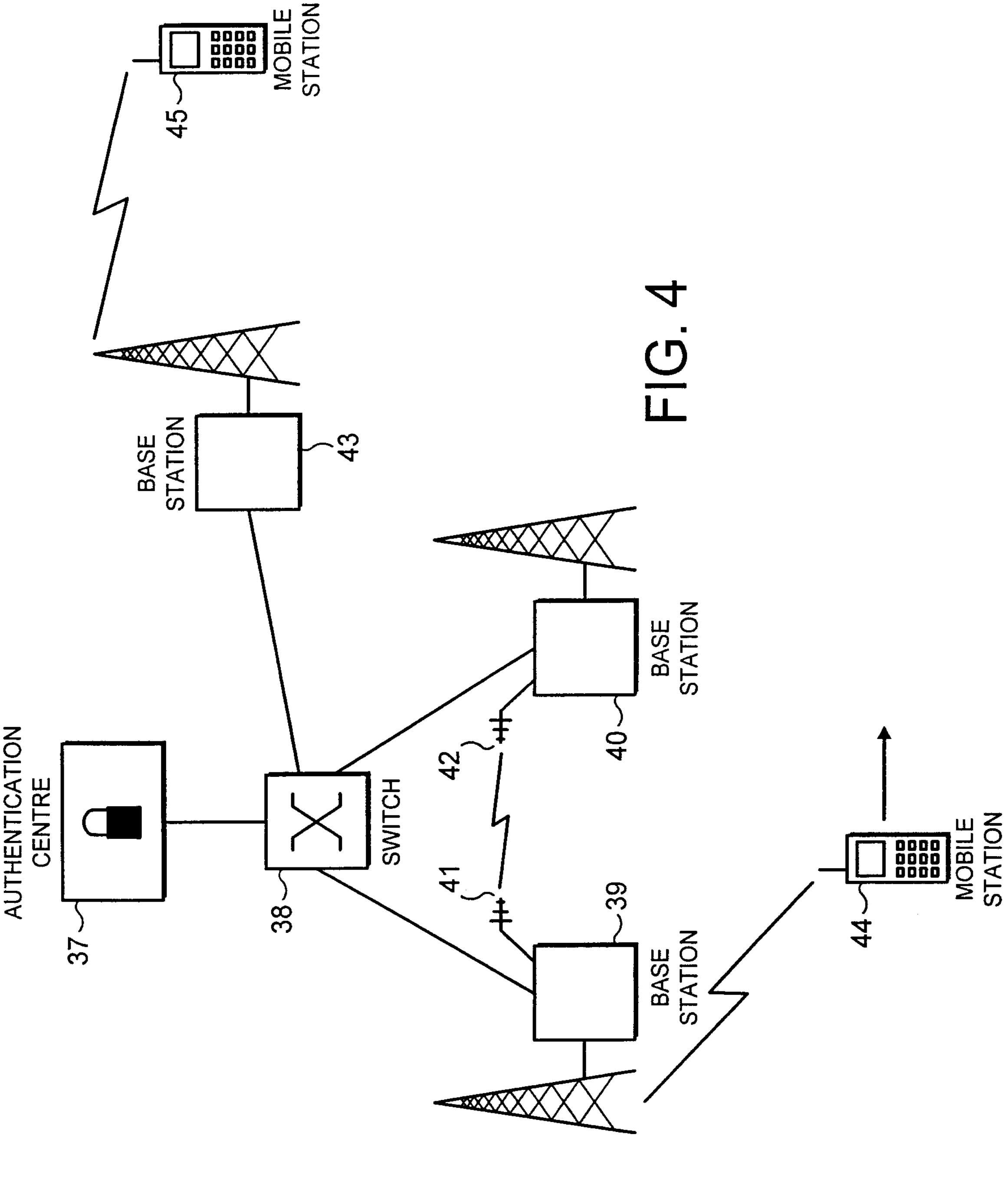

AUTHENTICATION CENTRE
37
SWITCH
38
BASE STATION
39
41
42
BASE STATION
40
BASE STATION
43
MOBILE STATION
45
MOBILE STATION
44

FIG. 4

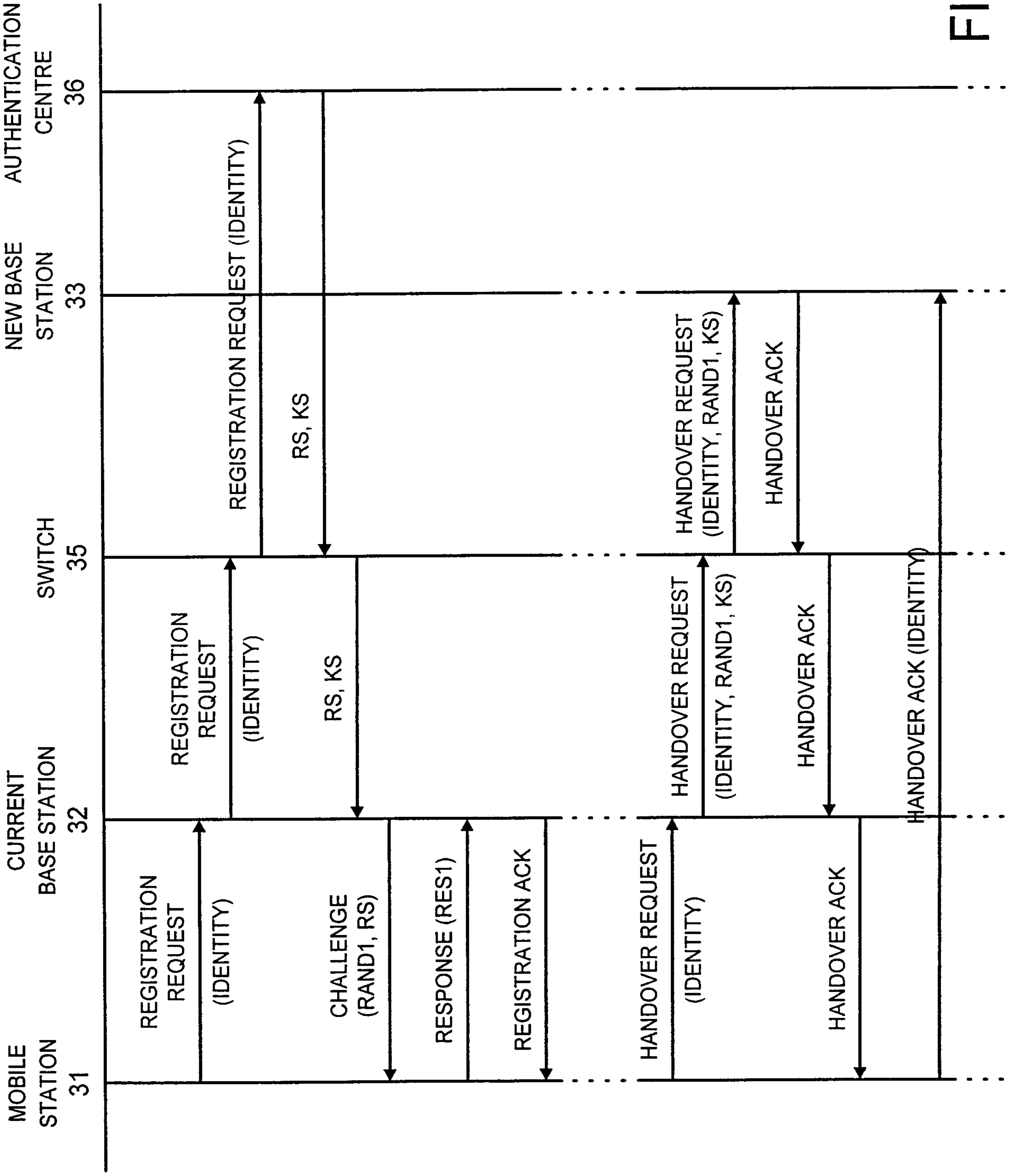

MOBILE STATION 31
CURRENT BASE STATION 32
SWITCH 35
NEW BASE STATION 33
AUTHENTICATION CENTRE 36
REGISTRATION REQUEST (IDENTITY)
REGISTRATION REQUEST (IDENTITY)
REGISTRATION REQUEST (IDENTITY)
RS, KS
RS, KS
CHALLENGE (RAND1, RS)
RESPONSE (RES1)
REGISTRATION ACK
HANDOVER REQUEST (IDENTITY)
HANDOVER REQUEST (IDENTITY, RAND1, KS)
HANDOVER REQUEST (IDENTITY, RAND1, KS)
HANDOVER ACK
HANDOVER ACK
HANDOVER ACK
HANDOVER ACK (IDENTITY)

FIG. 5

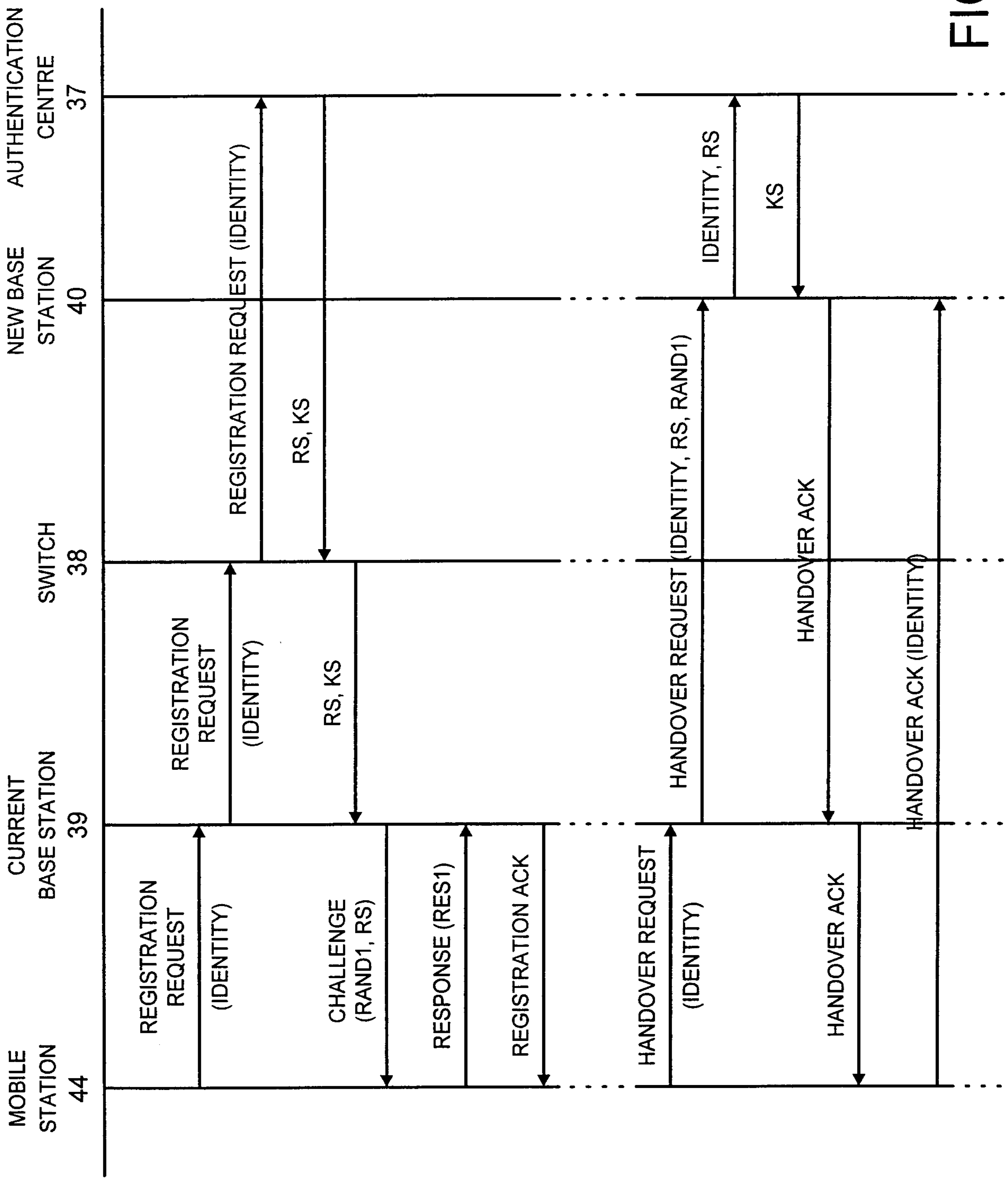

MOBILE STATION
44
CURRENT BASE STATION
39
SWITCH
38
NEW BASE STATION
40
AUTHENTICATION CENTRE
37
REGISTRATION REQUEST
(IDENTITY)
REGISTRATION REQUEST
(IDENTITY)
REGISTRATION REQUEST (IDENTITY)
RS, KS
RS, KS
CHALLENGE (RAND1, RS)
RESPONSE (RES1)
REGISTRATION ACK
HANDOVER REQUEST
(IDENTITY)
HANDOVER REQUEST (IDENTITY, RS, RAND1)
IDENTITY, RS
KS
HANDOVER ACK
HANDOVER ACK
HANDOVER ACK (IDENTITY)

FIG. 6

INTERNATIONAL SEARCH REPORT

Interr. nal Application No
PCT/GB 00/03702

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X A	WO 00 41427 A (ERICSSON TELEFON AB L M) 13 July 2000 (2000-07-13) page 2, line 25 -page 3, line 23 page 5, line 5 - line 26 page 6, line 12 -page 7, line 14 page 9, line 10 -page 10, line 15 ---	1-9,13, 14,16-22 10-12,15
A	US 5 598 459 A (HAARTSEN JACOBUS C) 28 January 1997 (1997-01-28) column 3, line 24 - line 36 column 5, line 60 -column 6, line 27 -----	1-22

□ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 14 December 2000	Date of mailing of the international search report 27/12/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Rothlübbers, C

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr. nal Application No
PCT/GB 00/03702

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0041427 A	13-07-2000	AU 2335300 A	24-07-2000
US 5598459 A	28-01-1997	AU 697775 B	15-10-1998
		AU 6396196 A	30-01-1997
		BR 9608791 A	17-02-1999
		CN 1193449 A	16-09-1998
		EP 0835594 A	15-04-1998
		JP 11508742 T	27-07-1999
		WO 9701943 A	16-01-1997